Basics

Note 1

21e64c2f0430467f8a36481045e172b3

{{c2::$\mathbb{Z}^+$, $\mathbb{Q}^+$ and $\mathbb{R}^+$}} denote {{c1::the positive (nonzero) elements in $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$, respectively.}}

Note 2

ad32571de5d04cafb2a7d6a27aee4b14

Given a function $f : A \to B$, {{c1::the set B}} is called the codomain of f.

Note 3

0cd492ad876a4dfbbb22c9210039fcc1

Given a function $f : A \to B$ and {{c3::a $b \in B$,}} {{c2::the preimage of $\{b\}$ under f}} is called {{c1::the fiber of f over b.}}

Note 4

b2a02c66209140a591b43dede69ffbf1

If $f : A \to B$ and $g : B \to C$, then the {{c1::composite map}}

$$g \circ f : A \to C$$

is defined by

$$(g \circ f)(a) = g(f(a)).$$

Note 5

1b2bf2fe79dc4063a151a960f45698d9

A function $f : A \to B$ {{c3::has a left inverse}} if there is a function $g :$ {{c2::$B \to A$}}, such that {{c1::

$$g \circ f = id_A.$$

}}

Note 6

d9a63bd7866e44ab83172cf9189e9b9a

A function $f : A \to B$ {{c3::has a right inverse}} if there is a function $g :$ {{c2::$B \to A$}}, such that {{c1::

$$f \circ g = id_B.$$

}}

Note 7

8098015b57774529a721663e39eabb18

A map f is {{c1::injective}} if and only if f has a {{c2::left}} inverse.

Note 8

205100b0fd6447a9bcc94e4d7711a606

A map f is {{c1::surjective}} if and only if f has a {{c2::right}} inverse.

Note 9

8e4ddf27550f4aa9a1daf0b67cd2f7e4

A {{c2::permutation}} of a set A is {{c1::a bijection from A to itself.}}

Note 10

1feef80fbcdd48618084ce93c88df83b

If $A \subseteq B$ and $f : B \to C$, {{c2::the restriction of f to A}} is denoted {{c1::$f|_A$.}}

Note 11

01a5a3b0e5f24f6782e689090b17c437

If $A \subseteq B$ and $g : A \to C$ and there is a function $f : B \to C$ such that {{c2::$f|_A = g$,}} we shall say f is {{c1::an extension of g to B.}}

Note 12

6ca7e478954c4c898718ce116219822f

{{c2::A binary relation on a set A}} is {{c1::a subset R of $A \times A$.}}

Note 13

50bb82cd97cb40bf8621065845545d18

Let R be a binary relation on a set A. We write {{c2::$a \sim b$}} if {{c1::$(a, b) \in R$.}}

Note 14

65287096376a47f399a0048c0d8092d0

A binary relation R on A is said to be {{c2::reflexive}} if {{c1::

$$a \sim a, \text{ for all } a \in A.$$

}}

Note 15

71b961a1f8f347dcbf7b9c7c8dee303c

A binary relation R on A is said to be {{c2::symmetric}} if {{c1::

$$a \sim b \text{ implies } b \sim a \text{ for all } a, b \in A.$$

}}

Note 16

40964931d9594b2997437cc9e3e150cc

A binary relation R on A is said to be {{c2::transitive}} if {{c1::

$$a \sim b \text{ and } b \sim c \text{ implies } a \sim c \text{ for all } a, bc \in A.$$

}}

Note 17

54a959a8e36045c1aea2d838ce8998b8

A binary relation is {{c2::an equivalence relation}} if {{c1::it is reflexive, symmetric and transitive.}}

Note 18

7c28d643ddd74509b88cfe2f75e6d743

If $\sim$ defines an {{c3::equivalence}} relation on A, then {{c2::the equivalence class}} of $a \in A$ is defined to be {{c1::

$$\{x \in A \mid x \sim a\}.$$

}}

Note 19

323fae73cd4b47ddb8c19cb515ffd4cf

If C is an equivalence class, {{c2::any element of C}} is called {{c1::a representative of the class C.}}

Note 20

3a597e1d5c48420490d792b972a38fe6

{{c2::A partition of a set A}} is {{c3::any collection $\{A_i \mid i \in I\}$ of nonempty subsets of A}} such that {{c1::A is the disjoint union of all A_i.}}

Note 21

c2216701429649b7a262afdd5c85a72d

If $\sim$ defines an equivalence relation on A then {{c2::the set of equivalence classes of $\sim$}} form {{c1::a partition of A.}}

Properties of the Integers

Note 1
f535d29c343f494fa35bccefce9d6988

Let $a, b \in \mathbb{Z}$. We write {{c2::$a \mid b$}} if {{c1::a divides b.}}

Note 2
96293ae3b76348d8ba9f0b02c8b49a94

Let $a, b \in \mathbb{Z}$ with $a \neq 0$. We write {{c2::$a \nmid b$}} if {{c1::a does not divide b.}}

Note 3
533403fe830341a39cee216314b861e8

Let $a, b \in$ {{c3::$\mathbb{Z} - \{0\}$ }}. {{c2::The greatest common divisor of a and b}} is denoted by {{c1::(a, b).}}

Note 4
20b204b896884b6b9d07ca3023b7cf4a

Let $a, b \in$ {{c3::$\mathbb{Z} - \{0\}$ }}. If {{c2::$(a, b) = 1$,}} we say that a and b are {{c1::relatively prime.}}

Note 5
69adfe8820204997a5aa44c50b353a40

If $a, b \in \mathbb{Z} - \{0\}$, then there exists unique $q, r \in \mathbb{Z}$ such that

$$a = qb + r \text{ and } 0 \leqslant r < |b|,$$

where q is {{c1::the quotient}} and r {{c1::the remainder.}}

«{{c2::Division Algorithm}}»

Note 6
6267be99c4884a09b1282d041ac05e18

If $a, b \in \mathbb{Z} - \{0\}$, then there exist $x, y \in$ {{c3::$\mathbb{Z}$}} such that

$${{c2::(a, b)}} = {{c1::xa + yb.}}$$

Note 7
e30ea564f2ce479391e71512867aea51

If p is prime and $p \mid ab$, for some $a, b \in \mathbb{Z}$, then {{c1::

$$\text{either } p \mid a \text{ or } p \mid b.$$

}}

Note 8

3cc931ead0ec4cddae21114d84f1de0c

{{c3::The Euler φ-function}} is defined as follows: for $n \in$ {{c2::$\mathbb{Z}^+$}} let $\varphi(n)$ be {{c1::the number of positive integers $a \leq n$ with a relatively prime to n.}}

Note 9

03f37e11eb9d40d29ca92031ac27d9ed

Let φ stand for the Euler φ-function. If p is {{c3::prime}} and $a \geq 1$, then

$${{c2::\varphi(p^a)}} = {{c1::p^a - p^{a-1}.}}$$

Note 10

7dc766a783c04a309951678711bd8317

Let φ stand for the Euler φ-function. Then

$${{c1::\varphi(ab) = \varphi(a)\varphi(b)}} \quad \text{if } {{c2::(a,b) = 1.}}$$

The Integers Modulo n

Note 1

76ca1b2698d942d599ad48365f1f326d

Let {{c3::$n \in \mathbb{Z}^+$.}} Then {{c2::a is congruent to b mod n}} if {{c1::

$$n \mid (b - a).$$

}}

Note 2

b9af5bdff0c74d4caef2f944b60a0e0f

Let $n \in \mathbb{Z}^+$. If {{c2::a is congruent to b mod n,}} we write {{c1::

$$a \equiv b \pmod{n}.$$

}}

Note 3

621ea0d4d5b34a1dba53213679217108

Let $n \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$. {{c1::The equivalence class of a with respect to congruence mod n}} is {{c2::called the congruence class or residue class of a mod n.}}

Note 4

ae25b5393fbf40e0b4cf815ff226d2c2

Let $n \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$. {{c2::The congruence class of a mod n}} is denoted {{c1::$\bar{a}$.}}

Note 5

b8d65811b13a46b9b3053adfd435278a

Let $n \in \mathbb{Z}^+$. There are {{c1::precisely n}} distinct equivalence classes mod n.

Note 6

2d8fe349d9fd4243a25995a4854b9678

Let $n \in \mathbb{Z}^+$. {{c1::The set of equivalence classes under the relation of congruence mod n}} is denoted by {{c2::

$$\mathbb{Z}/n\mathbb{Z}.$$

}}

Note 7

f35ce536d04d4ac881f916866b6cec8f

Let $n \in \mathbb{Z}^+$. The set $\mathbb{Z}/n\mathbb{Z}$ is called {{c1::the integers modulo n.}}

Note 8

42a30108f0414522b336bfb5ed2d767a

Let $n \in \mathbb{Z}^+$. The process of {{c2::finding the equivalence class mod n of some integer a}} is often referred to as {{c1::reducing a mod n.
}}

Note 9

f6a8649b8e80420baaa019f8fbf718f4

Let $n \in \mathbb{Z}^+$. {{c1::The smallest non-negative integer congruent to a mod n}} is called {{c2::the least residue of a mod n.}}

Note 10

ae2d3fee4b4e492f9c5c9f0f81bad35c

Let $n \in \mathbb{Z}^+$ and $\bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$. Then

$$\text{\{\{c2::}\bar{a} + \bar{b}\text{\}\}} \stackrel{\text{def}}{=} \text{\{\{c1::}\overline{a + b}.\text{\}\}}$$

Note 11

5952ca056a4b483c8f5bb5cb3b196378

Let $n \in \mathbb{Z}^+$ and $\bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$. Then

$$\text{\{\{c2::}\bar{a} \cdot \bar{b}\text{\}\}} \stackrel{\text{def}}{=} \text{\{\{c1::}\overline{ab}.\text{\}\}}$$

Note 12

ebb13f63a9be46ff9ab758d279644ae8

Let $n \in \mathbb{Z}^+$. {{c2::$(\mathbb{Z}/n\mathbb{Z})^\times$}} $\stackrel{\text{def}}{=} \{\bar{a} \mid$ {{c1::there exists $\bar{c}$ with $\bar{a} \cdot \bar{c} = \bar{1}$}}$\}$.

Note 13

866ff8df0c6d4a589ee1a49fb58fb15e

Let $n \in \mathbb{Z}^+$. Then

$$\text{\{\{c2::}(\mathbb{Z}/n\mathbb{Z})^\times\text{\}\}} = \{\bar{a} \mid \text{\{\{c1::}(a, n) = 1\text{\}\}}\}.$$

Note 14

aeffe5fd9f8f4f658853ad5cf6dada0a

Let $n \in \mathbb{Z}^+$. Then $(a, n) = 1$ implies $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. What is the key idea in the proof?

> Represent (a, n) as a $\mathbb{Z}$-linear combination of a and n.

Note 15

c238e2ff17e84fd98c1adec56082e6c4

Let $n \in \mathbb{Z}^+$. Then $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ implies $(a, n) = 1$. What is the key idea in the proof?

> By contradiction and multiply $ac \equiv 1$ by $\frac{n}{(a,n)}$.

Note 16

31261830ed6b43549a4f35afc29785a9

Let $n \in \mathbb{Z}^+$. The number of elements in $(\mathbb{Z}/n\mathbb{Z})^\times$ is {{c1::$\varphi(n)$ where φ denotes the Euler φ-function.}}